Mobile Services Category Team (MSCT)

A Call to Action

Bring Your Own Device (BYOD)

Personally-Owned, Government-Enabled Devices

May 2019

INTRODUCTION

Since the advent of smartphones and tablets, those responsible for remote access to federal systems have been challenged with getting enterprise mobility policies written/approved, acquiring/configuring appropriate security features and updating agency network access to manage the risk and respond to evolving needs of the modern workforce. It is no surprise that most companies allow their employees to access business systems from their personally-owned smartphones or tablets. Likewise, in the federal sector senior executives and agency managers are expected, at least, to check (unclassified) email and access electronic calendar on the go. Virtually all agencies manage a mobile device provisioning program to provide a portion of their workforce with government furnished equipment (GFE). Increasingly executives, mid-level managers, and others are using personally-owned smartphones or tablets to access agency systems/data.

Agency enterprise mobility programs can generally be described as:

- **Fully managed** – In this deployment scenario, devices are typically owned by the agency, locked down and only permitted to perform business functions. These devices are centrally managed which provides important security benefits, but also presents usability barriers to employees. Fully managed devices are GFE and all data residing on the device is owned by the government, necessitating that employees have a second device for personal use.
- **Personally Owned, Government Enabled** – Devices are owned by the end-user but occasionally are used for work, and should be permitted the least access to organization resources. These devices are typically joined directly to a Mobile Device Manager (MDM) with end-user consent, but are more often managed through a mail and calendaring system such as Exchange ActiveSync. Access from BYOD devices to organizational resources should be strictly controlled and limited.
- **Unmanaged** – Organizations provide access to enterprise services, such as email, contacts, and calendar, to employee users without surveying or inspecting the device. This is the most dangerous scenario to the enterprise and should be avoided to the extent possible.

As we near the end of the second decade after the millennium, Bring Your Own Device (BYOD) has become a de facto part of work life balance in today's digital society. This paper will:

1. **Identify official federal BYOD Guidance**
2. ***Provide criteria for initial analysis of risks, costs, and benefits of a program for personally owned, government enabled devices***
3. ***Provide guidance on protecting/separating agency data from personal data and how to deal with spillage***
4. ***Explain roadblocks to offering employee reimbursement of costs incurred when using a personally owned device***
5. ***Outline reasons why agency leadership often shy away from supporting a program with personally owned devices***

The concluding remarks form a "Call to Action" for agency executives to understand the tradeoffs in implementing a Personally Owned Government Enabled BYOD program and terminate unmanaged BYOD programs which serve to undermine the security of enterprise mobility programs.

I. FEDERAL BYOD GUIDANCE TO DATE (SEE APPENDIX FOR SUMMARY)

In 2019 the Center for Internet Security (CIS) published CIS Controls Mobile Companion Guide which provides government with a consistent approach on how to apply the CIS Controls security recommendations to Google Android and Apple iOS environments. Factors such as "*Who owns the data?*" and "*Who owns the device?*" all affect how the device can be secured, and against what threats. The guide explores various ways that organizations purchase, provision, and provide mobile devices to employees. Styles include bring your own device (BYOD), Government-owned, personally-enabled, fully managed, and unmanaged.

In 2018, the General Services Administration (GSA), Mobile Services Category Team (MSCT) and the ATARC Mobility Work Groups jointly updated federal BYOD Guidance. The 2018 Federal BYOD Guidance was posted on GSA Acquisition Gateway in May of 2018. This material reflects thought leadership among current federal BYOD practitioners, product/service providers and academics. The Updated BYOD Guidance includes three case studies: Nuclear Regulatory Commission (NRC), Navy Reserve – Ready2Serve (R2), US Equal Employment Opportunity Commission (EEOC). Note that none of the BYOD programs discussed in these case studies involve the transmission of classified information. Agencies should consider the applicability of the technical and policy approaches contained in the case studies to their own environments.

In 2016 GAO issued an opinion affirming that agencies may expend resources to support a program for BYOD. As Federal New Radio's Jason Miller reported, *"GAO ruled on Feb. 19, 2016, that the Consumer Product Safety Commission's (CPSC) voluntary BYOD program for its employees doesn't violate any appropriations or gift laws, and the agency can provide technical support to its workers" There were several outstanding questions, ranging from could the government pay employees a stipend or share somehow in the expense of the phone costs, to whether the mobile device management (MDM) systems are good enough to keep federal and personal data separate, to the whole idea of developing government apps.CPSC's voluntary BYOD program is neither an augmentation of appropriations nor a gift, and CPSC may use appropriated funds to support the program," GAO said in its ruling. "As indicated, an agency's compliance with the miscellaneous receipts statute is but one of the many relevant considerations applicable to a program such as that contemplated by CPSC."*

Many agencies believe that staying with government-furnished devices makes the most sense. The GAO decision is important because it gives agencies more confidence that even without the ability to reimburse employees, offering them the option to use their own smartphones or tablet computers provides the potential for real savings. This was the first ruling by GAO on an agency's BYOD program, thus setting a precedent for agencies as they decide how to evolve their enterprise mobility programs.

Also in 2016, NIST issued Special Publication SP 800-114 Rev 1 (July 2016) **User's Guide to Telework and Bring Your Own Device Security**: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf and a companion document called ***Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security***. See SP 800-46 Rev 2 (July 2016): http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

In 2013, NIST issued ***Guidelines for Managing the Security of Mobile Devices in the Enterprise,*** NIST Special Publication (SP) 800-124 Revision 1. It helps organizations centrally manage and secure mobile devices against a variety of threats, providing recommendations for selecting, implementing, and using centralized management technologies, and explaining the security concerns inherent in mobile device use. The scope of SP 800-124 Revision 1 includes securing both organization-provided and personally-owned (bring your own device) mobile devices. NIST is planning an update of SP800-124 during 2019.

Later in 2012, the EEOC's BYOD pilot program was the featured cover story for Fed Tech Magazine Fall 2012, ***Bring IT!,*** which outlined the potential for cost savings, attention needed for staff training, the criticality of collaboration between agency IT, CFO, Legal and HR leadership. BYOD became a popular discussion topic at mobility conferences and thought leadership events. A number of agencies launched BYOD work groups, pilot programs, and research into how private sector companies were dealing with BYOD.

Data Explosion Poses Storage Challenges 26
Federal Cloud Efforts Adopt the Private Model 30
Defend Your IT Enterprise Against Botnets 12
FEDTECH™
Technology Insights for Leaders in Federal Government
fedtechmagazine.com
Treating Military Hospitals' Woes with Voice Recognition 18
Video Learning Drives Education 24
BRING IT
Agencies Explore Their BYOD Options 20
EEOC's Kimberly Hancher oversees one of the federal government's first BYOD programs.
FALL 2012
CDWG

The first federal BYOD guidance, for agencies to consider the voluntary use of personally-owned, government-enabled mobile wireless devices for federal government business, was published by the Obama Administration in May 2012. The 2012 Federal BYOD Guidance and Toolkit provides Federal IT organizations with criteria to determine whether BYOD might be appropriate for their agency, sample BYOD policies, and rules of behavior for federal employees/contractors using their personal smartphones or tablets on a voluntarily basis, (i.e., not as a condition of work). The Toolkit also included two case studies of federal agency BYOD programs: EEOC and the Alcohol Tobacco Tax and Trade Bureau, and a case study of BYOD in the state of Delaware.

In addition to the above listed federal BYOD guidance, the final page of this document provides a table of constitutional and statutory references associated with BYOD.

Call to Action: Agency IT leaders should ensure that their government and contractor workforce responsible for the agency enterprise mobility management programs are familiar with the publications listed and are using the material to inform decisions about enterprise mobility programs.

II. TO BYOD OR NOT TO BYOD, THAT IS THE QUESTION!

Consideration of a BYOD program for any agency must ensure that it fits the agency's security posture, integrates into its operational environment, supports its mission goals and requirements, and meets the needs of its staff. The 2018 Updated BYOD Guidance is clear that **BYOD is not intended, nor is expected, to be a good fit for all agencies.** The burden falls on agency leadership to heed this call to action to decide whether BYOD is appropriate or not, for their workforce.

Federal executives (CIO, CFO, COO, GC, CISO) are urged to consider the risks, costs and benefits of establishing a BYOD program.

1. Agencies should conduct an initial risk analysis focused on the sensitivity of data which might be made available to the BYOD participants. An initial risk analysis should consider:
    - **Classified Data** – Does the agency have any classified data stored in the systems that BYOD users would access? If the answer is no, move on to the next area of consideration. If the answer is yes, additional risk analysis is needed.
    - **Sensitive Personally Identifiable Information (PII)** – Does the agency have any sensitive PII data stored in the systems that BYOD users would access? If the answer is no, move on to the next area of consideration. If the answer is yes, additional risk analysis is needed.
    - **Sensitive But Unclassified (SBU) data** – Does the agency's network/systems have SBU data that might be of interest to terrorists, adversaries or bad actors? If the answer is no, move on. If the answer is yes, additional risk analysis is needed.
    - **Law Enforcement Case Data** - Does the agency's personnel collect data that might be related to law enforcement cases? If the answer is no, move on. If the answer is yes, additional risk analysis is needed.

    If the answer to any of the above questions is yes, then additional risk analysis should be conducted to determine the likelihood and impact if sensitive data is spilled or otherwise compromised.

    If the answer to all four questions in the initial risk analysis is no, then the agency should move forward in evaluating the costs and benefits of a BYOD program for the agency.

2. Agencies should also consider the "business case" for implementing a BYOD program. A preliminary economic analysis or cost benefit study that outlines the expected value (employee productivity, morale, flexibility, proficiency with mobile device, new enterprise service) versus cost (impact on help desk, training, staffing, etc) will vary from agency to agency.

<u>Call to Action:</u> Has your agency conducted an analysis on whether BYOD is appropriate or not for the workforce? Agencies should conduct an initial risk analysis focused on the sensitivity of data which might be made available to the BYOD participants. Once the agency has composed its position on the topic, engage/inform agency leadership, mid-level managers and employees. As appropriate, analyze the business case for personally owned government enabled devices, update end user rules of behavior, network usage agreements, and any other documents that help end users understand the boundaries of using personally-owned devices for business purposes.

III. <u>PROTECTING/SEPARATING AGENCY DATA FROM PERSONAL DATA</u>

When implementing a program for managing personally owned devices, agencies must determine what security measures are in order. If employees will be accessing email and calendars, then agencies may only need to provide provisional protection on the device.

However, if personally owned devices are granted access to time/attendance systems, financial management systems, and / or other more sensitive data, more stringent security must be implemented. At a minimum, a

Mobile Device Management (MDM) solution provides agencies with the ability to push out, manage, and track agency containers on government-furnished and personally-owned devices. MDM administrators can quickly and easily manage those containers by (1) pushing IT & compliance policies directly to the device, (2) remotely wipe or removing the container from the device in the event of device compromise including if it's lost or stolen, and (3) control what type of resources a user is allowed to access within the container. To delineate the boundary between agency data and personal data, it is suggested that agencies employ MDM solutions that allow them to deploy their resources to personally owned devices via a managed container or device-level work profile.

- **Managed Container -** allows the agency to create a sandboxed environment on the device which logically separates the agency resources and data from the rest of the device, typically personal data.
- **Device Level Work Profile/Persona -** Similar to the containerization solution, these solutions create a logically separated work profile that acts as a second persona on the device complete with its own suite of work-related applications and policies that can be managed by agency IT while still allowing the employee to conduct personal business on the personal half of the device.

The key differences between a managed container solution vs. a device work profile is that a containerization approach typically involves the installation of an app or series of apps that take advantage of the devices natural sandboxing architecture for keeping installed apps from interacting with system files. Device-level work profile solutions create a second, logically separate persona on the device that allows employees to have personal and work-related applications on the same device that do not speak or see each other. For example, a single device could have a personal Gmail account and a work-related Gmail account that can be accessed separately and do not overlap. This approach allows the user to access and conduct work directly on their device but prevents apps and resources from the personal side of the device from accessing the work data. Both solutions provide agency IT administrators with a clear delineation line between employee personal data and work data that might exist on the device to secure and remove should an issue arise.

When personally-owned devices are used for government business, what do you do if there is a spillage of information? DoD and DHS generally want to wipe the device if spillage occurs. However, wiping the device may wipe critical data needed for an after action analysis or investigation. In case of spillage, we recommend that agency policies, standard operating procedures and rules of behavior ensure that access to enterprise data be curtailed while analysis of the situation is conducted. Upon report of spillage, immediately power off the device and assess the situation. A personally-owned mobile device should not have sensitive or classified information on it, but if it does: Power the device off, put it in a Faraday bag, if possible, and address the situation based on agency policies and procedures. Device containers, described above, have decreased the need to fully wipe personally owned devices, offering agencies the option of conducting a partial wipe/selective wipe.

Call to Action: As you evaluate enterprise mobility software and solutions to support a BYOD program, select technology that will keep personal information separate from government resources/data on the device.

IV. BYOD REIMBURSEMENT

Mobility management for both private and public sector organizations today involves managing a mix of both personally-owned and government-owned devices. The biggest hurdle in reimbursing employees for BYOD lies in the details. In order to calculate compensation, an accurate log of business use of the device must be tracked. Beyond tracking employee hours, options for tracking business use are severely limited. That may explain why only 13% of employees receive any monetary reimbursement for BYOD, according to Forrester. Most companies don't reimburse employees for work-related use of their devices, and 54% of employees foot the tab for mobile data used for work. However, many cell phone plans now have unlimited data, talk and text, so more commercial companies are now providing reimbursement for a portion of the employee's phone bill. Since the government sometimes follows commercial best practices, developing a formula for the government to provide reimbursement for a portion of the data usage might be possible in the future.

The discussion about BYOD reimbursement in the federal sector has identified significant roadblocks when considering reimbursement for the cost of personally-owned devices used for government business:

- ***Legal Framework is disjointed***: At this time, there is an absence of "precedence" for establishing a federal BYOD reimbursement program. Federal counsel typically cites the GAO Decision on ***Reimbursing Employees' Government Use of Private Cellular Phones, B-287524, October 22, 2001.*** The agency, Western Area Power Administration (WAPA), requested an advanced decision from GAO on whether WAPA could reimburse employees for government use of personally-owned devices at a tiered flat rate based on historical usage. GAO had no objection to reimbursing employees, however, without specific statutory authority, *"an agency may not reimburse employees at a flat rate instead of reimbursing for actual expenses. Agency reimbursement must be based on the actual cost incurred by the employee for business use. The agency may not reimburse an employee based on an estimated, pre-determined, standard or negotiated amount."* Note that we always use the term *reimbursement* instead of *stipend, which is,* by definition, a predetermined amount of money that is provided periodically to help offset expenses. The aforementioned GAO Opinion is clear that a stipend is not acceptable.

- ***Identifying Actual Cost of Business Use is difficult***: Even agencies with comprehensive remote access security and the ability to track "approved" personally-owned device activity as a "business persona" have not implemented the ability to distinguish costs associated with "*business use*" vs "*personal use."*

Although the 2012 Federal BYOD Guidance and Toolkit included a case study on BYOD reimbursement in the State of Delaware, there is no federal precedent, at this time, for implementing reimbursement of costs associated with federal employees using their personally-owned devices for official business.

Call to Action: In establishing federal agency BYOD programs, agencies should make clear that the employee is personally responsible for all wireless service related costs of using their own device for government business. However, the government should budget for and bear the cost of the security they need to protect agency data.

V. EMPLOYEES ARE USING THEIR OWN DEVICES WHETHER YOU KNOW IT OR NOT!

Federal agency progress in developing a policy framework to offer their agency personnel the ability to perform some business-related tasks using their personally-owned devices has been very slow. A few of the biggest hurdles to BYOD in the federal sector include:

- **Risk Avoidance** - Given that federal executives tend to be much more risk averse than their colleagues in the private sector, it is not surprising that concerns about compromising security tops the list of hurdles. In an attempt to avoid the risk of introducing a program for BYOD, many agencies have remained silent on the topic. In fact, security risk is often used as a scapegoat for avoiding a decision on BYOD. Quite a few agencies, especially those that do not deal with classified data, have enabled remote access to official email, calendar, contacts and select other agency systems using personally-owned devices, but some of these agencies neglected to put in place a policy, program or rules of behavior.

- **Risk Acceptance –** Many agencies have drafted BYOD policy or are in "pilot" mode but never got final sign off on their BYOD program. Many agencies lack the support of an Executive Sponsor willing to move the BYOD program into place and sign off on acceptance of risk.

The primary reason cited for not adopting BYOD are "security concerns" but having the right networking infrastructure, device security, and management software can mitigate these concerns.

While a number of civilian and DOD agencies have researched and piloted voluntary BYOD programs, only a small proportion of federal agencies have produced a policy on using personally-owned devices to conduct federal business and promulgated rules of behavior for end users to support the new genre of personally owned government enabled devices. .

Unfortunately, most federal employees remain very confused about whether or not their agency allows BYOD because so few agencies have established a cogent program and made it available to their staff. Even agencies that have determined that a BYOD program should **not** be implemented have failed to include language restricting business use of personal smartphones and tablets in their standard RoBs for agency network end users. As of 2016, nearly 87% of companies rely on their employees using personal devices to access business apps (Syntonic). It is logical that new federal employees, fresh from working in the private sector or new to the workforce, expect clear guidance on acceptable uses of personal devices.

While many agencies provide remote access to email, internal calendars, and contacts for employees with personally-owned smartphones and tablets*,* most agencies do not document the program in plain language, nor do they codify the ROBs specific to using a personal device to access federal systems. Many agency employees remain uncertain about whether they are permitted to use their personal devices for work. In fact, in a recent study of federal employees showed nearly 40% were not sure whether or not their agency permits the use of personally-owned devices to access agency data.

At one end of the spectrum agencies like the State Department,; State Department civilian employees are clear that personal wireless devices may **not** be used to access State Department systems and are not allowed in areas where classified business is conducted. At the other end of the spectrum agencies like Nuclear Regulatory Commission (NRC) have issued clear BYOD guidance and rules of behavior for its BYOD program.

Call to Action: If your agency does not support BYOD, update your agency standard Network Rules of Behavior to document the restrictions against using personal devices for business use. If you offer a BYOD program, update agency network rules of behavior to identify acceptable uses. Agencies must put policies and expected rules of behaviors (ROB) in place to ensure users understand what they are allowed to do and not do with agency resources vis-à-vis a personal device.

CONCLUDING REMARKS

Too many agencies have not yet driven closure on the question ***TO BYOD or NOT TO BYOD?*** More agencies should be interested in establishing a BYOD program. According to a 2015 survey of more than 1,000 federal employees, 50% of federal employees use their personal devices for work email, while 49% said they download government data to their personal devices. The survey suggests many agencies already have a "shadow BYOD" program because employees are using their personal devices for work without proper security controls. The time has come to push agencies to recognize the existence of these "shadow" programs and put some rigor and cyber controls in place.

Government leaders should heed these ***Calls to Action***:

1. **Use available BYOD guidance and reach out to your colleagues in the federal BYOD community of practice.**
2. **Conduct an initial analysis of risks, costs, and benefits. Determine whether a BYOD personally owned, government enabled device program is appropriate or not for your agency's workforce.**
3. **Determine the right tools and approach to securely separate government/agency data from personal data.**
4. **In establishing federal agency BYOD programs, agencies should make clear that the employee is personally responsible for all wireless service-related costs of using their own device for government business.**
5. **If your agency does not support BYOD, update your agency standard Network Rules of Behavior to document the restrictions against using personal devices for business use. If you offer a BYOD program, update agency network rules of behavior (ROB) to identify acceptable uses. Agencies must put policies, training and expected ROBs in place to ensure users understand what they are allowed to do and not do with agency resources vis-à-vis a personal device.**

APPENDIX

Federal Guidance, NIS&T Special Publications (SP) and Other Publications on Federal BYOD

2018 Federal BYOD Guidance	https://hallways.cap.gsa.gov/system/files/MSCT%20BYOD%20Guidance%20Report%20FINAL%20-%203May2018-1530555996.docx
CIS Controls Mobile Companion Guide	https://www.cisecurity.org/blog/new-release-cis-controls-mobile-companion-guide/
SP 800-46 Rev 2 (July 2016)	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
SP 800-114 Rev 1 (July 2016)	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
SP 800-124 Rev 1 (update in progress)	https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final
2012 Federal BYOD Guidance + Toolkit	https://obamawhitehouse.archives.gov/digitalgov/bring-your-own-device

Constitutional, Legislative, Statutory, Administrative Law References Relevant to Federal BYOD

4thand 5th Amendment of the Constitution	4th Amendment: Guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction. This protects individuals from illegal search and seizure by the Government. 5th Amendment: A citizen cannot be compelled or forced to testify against themselves in criminal proceedings. The Government may not deprive citizens of "life, liberty, and prosperity" without due process of law.
Electronic Communications Privacy Act of 1986 (18 USC § 2510 et set)	Prohibits the unauthorized interception or access to stored electronic communications and records. This confirms and protects an individual's expectation of data as it is electronically transmitted.
Privacy Act of 1974, 5 § USC 552a	A collection of additional information about the "users device" is required for provisioning and accountability.
Section 208 of the E-GOV Act of 2002 – Privacy Impact Assessment (PIA)	A PIA must be conducted and made publicly available before developing or procuring information technology to collect, maintain, and disseminate information about an individual's device.
E-Discovery and the Freedom of Information Act	The Government is required to provide all electronically stored information.
Stored Communications Act 18 U.S.C. Chapter 121 § 2701 - 2712	Enacted as part of the Electronic Communications Privacy Act. It protects data after it has completed transfer to a remote storage device
DoD 5500.7-R Joint Ethics Regulation Change 7 § 2-301 Use of Government Resources	Federal Government communications systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only.
Records management that applies to personal email	Current DoD policy prohibits the use of personal email to conduct official government business.